DATE(S) ISSUED:
09/27/2012

SUBJECT:
Multiple Denial of Service Vulnerabilities in Cisco Products

OVERVIEW:
Multiple vulnerabilities have been discovered in several Cisco products including Cisco Catalyst 4500E Series Switches, Cisco devices running Cisco IOS and Cisco IOS EX, as well as Cisco's Unified Communications Manager.
Successful exploitation of these vulnerabilities could result in denial of service conditions or reboot the affected device.

SYSTEMS AFFECTED:
   Cisco Catalyst 4500E Series Switch with Cisco Catalyst Supervisor Engine 7L-E
   Cisco IOS
   Cisco IOS EX 3.2.xXO
   Cisco Unified Communications Manager 6.x, Cisco Unified Communications Manager 7.x, Cisco Unified Communications Manager 8.x

RISK:
Government:
   Large and medium government entities: **High**
   Small government entities: **High**
Businesses:
   Large and medium business entities: **High**
   Small business entities: **High**
Home users: N/A

DESCRIPTION:
Multiple Cisco products are vulnerable to a remote Denial of Service condition. The details of each vulnerable Cisco product are provided below.

Cisco Operating Systems
The Cisco operating systems affected by these vulnerabilities are Cisco IOS and Cisco IOS EX, which run on a variety of Cisco networking devices. To determine if your version of IOS is affected, please visit the following site: http://tools.cisco.com/security/center/selectIOSVersion.x

To exploit these vulnerabilities, an attacker needs to create a specially crafted packet that, when processed, may result in the denial of service conditions. The details of the vulnerabilities are as follows:
   Improper handling of a malformed attribute from a peer on an existing BGP session can cause all BGP sessions to reset and to cause an inability to route packets to BGP,
   resulting in a denial-of-service condition. This issue is being tracked by Cisco bug IDs CSCtt35379, CSCty58300, CSCtz63248, and CSCtz62914(CVE-2012-4617).
   Improper handling of a specially crafted DHCP packet by the Device Sensor feature inCisco IOS can cause

the device to crash, resulting in a denial-of-service condition.
This issue being tracked by Cisco bug ID CSCty96049 (CVE-2012-4621).
Improper handling of a specially crafted packet sent to a device running a vulnerable version of Cisco IOS configured with DHCP version 6 may cause the DHCP server to
crash, resulting in a denial-of-service condition. This issue is being tracked by Cisco bug ID CSCto57723 (CVE-2012-4623)
Improper handling of a specially crafted DNS (Domain Name System) packet sent to a device running a vulnerable version of Cisco IOS with an affected Cisco IOS IPS
configuration can cause the device to reload, resulting in a denial-of-service condition. This issue is being tracked by Cisco Bug ID CSCtw55976 (CVE-2012-3950).
Improper handling of a specially crafted UDP Session Initiation Protocol (SIP) packet sent to port 5060 on a device running a vulnerable version of Cisco IOS with the NAT
SIP ALG feature enabled can cause the device to reload, resulting in a denial-of-service condition. This issue is being tracked by Cisco bug ID CSCtn76183 (CVE-2012
4618).
Improper handling of a specially crafted SIP message that contains a valid Session Description Protocol (SDP) message sent to a device running a vulnerable version of
Cisco IOS EX, which is configured to process SIP messages and for pass-through of Session Description Protocols (SDP) can cause the device to reload, resulting in a
denial-of-service condition. This issue being tracked by Cisco bug IDs CSCtj33003, CSCtw84664 and CSCtw66721 (CVE-2012-3949).
Improper handling of specially crafted ingress IP tunneled packets sent to a device running a vulnerable version of Cisco IOS may consume all available space in the
affected interface queue, resulting in a denial-of-service condition. This issue is being tracked by Cisco bug ID CSCts66808 (CVE-2012-4620).

Cisco Catalyst Switches
Cisco Catalyst Switches are Cisco's network switch product line of modular and fixed configuration switches.

4500E Series Switches with Cisco Catalyst Supervisor Engine 7L-E are prone to a remote Denial of Service vulnerability. To exploit the vulnerabilities, an attacker needs to
create a specially crafted packet that, when processed, may result in a denial of service condition. This issue being tracked by Cisco bug ID CSCty88456 (CVE-2012-4622).

Cisco Unified Communications Manager
Cisco Unified Communications Manager is the call-processing component of the Cisco IP Telephony solution that extends enterprise telephony features and functions to packet telephony network devices, such as IP phones, media processing devices, VoIP gateways, and multimedia applications.

To exploit the vulnerabilities in the Cisco UCM, an attacker needs to create a to reload specially crafted packet that, when processed, may result in the denial of service conditions. The details of the vulnerabilities are as follows:
Improper handling of a specially crafted SIP message that contains a valid Session Description Protocol (SDP) message sent to a device running a vulnerable version of
Cisco UCM, which is configured to process SIP messages and for pass-through of Session Description Protocols (SDP) can cause the device to reload, resulting in a denial
of-service condition. This issue being tracked by Cisco bug IDs CSCtj33003, CSCtw84664 and CSCtw66721 (CVE-2012-3949).

RECOMMENDATIONS:

The following actions should be taken:

· Upgrade vulnerable Cisco products immediately after appropriate testing.

REFERENCES:

Cisco:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-ecc
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-dhcpv6
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-dhcp
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-sip
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-cucm
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-c10k-tunnels
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-ios-ips
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-bgp
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-nat

SecurityFocus:

http://www.securityfocus.com/bid/55701
http://www.securityfocus.com/bid/55700
http://www.securityfocus.com/bid/55699
http://www.securityfocus.com/bid/55696
http://www.securityfocus.com/bid/55695
http://www.securityfocus.com/bid/55694
http://www.securityfocus.com/bid/55693

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4617
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4618
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4620
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4621
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4623
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3949
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3950